Candidate Information

Position:	Research Fellow - Federate Learning Security
School/Department:	School of Electronics, Electrical Engineering and Computer Science
Reference:	25/112711
Closing Date:	Sunday 10 August 2025
Salary:	£41,519 per annum.
Anticipated Interview Date:	Monday 18 August 2025
Duration:	12 months

JOB PURPOSE:

Federated learning (FL) is a privacy-preserving distributed learning paradigm that allows different clients to create a shared AI models without having to share their data. Despite these advantages, conventional FL frameworks are not exempt of security weaknesses. The role involves performing research to create on decentralised federated learning that 1) improved robustness against poisoning and adversaries whilst 2) while maintaining their privacy preserving properties.

Specifically, the role will involve investigating:
- Decentralised FL convergence and vulnerabilities.
- Novel decentralised robust aggregation technique considering local consensus by clustering the nodes based on similar data distribution.
- Novel decentralised robust aggregation technique considering local consensus by clustering the nodes based on local trust and consensus.

MAJOR DUTIES:

1. Undertake high-quality and novel research in the areas of AI agentic systems, excessive agency, misuse, sensitive data exposure, and supply chain assurance.
2. Design, develop, and refine experiments to evaluate anomaly detection performance.
3. Carry out analyses, critical evaluations, and interpretations using methodologies and other techniques appropriate to AI security.
4. Present regular progress reports on research to members of the research group or to external audiences to disseminate and publicise research findings.
5. Prepare, often in consultation with the line manager, material for publication in national and international journals and presentations at international conferences such as IEEE Security and Privacy, ACM in Computers and Communication Security.
6. Produce high-quality research outputs consistent with project aims and commensurate with the career stage.
7. Undertake supplementary duties relevant to the success of the project including administrative duties and additional training and development activities as required.

ESSENTIAL CRITERIA:

1. Have or about to obtain a PhD in computer science, engineering, mathematics or physical sciences area.
2. Recent high quality research experience in machine learning/AI, or both, as evidenced by a strong track record of publications in leading journals and conferences in relevant areas.
3. Software programming skills.
4. A consummate team player who is openminded and is prepared to work closely with other members of a large multidisciplinary research and development team, as well as with industrial collaborators.
5. Able to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.
6. On-site presence required in accordance with QUB policy (currently for a minimum 3 days per week).

DESIRABLE CRITERIA:

1. Normally have or be about to obtain a PhD in the area of machine learning/AI, cyberAI or distributed systems.

2. Hands-on experience in federated/distributed learning.
3. Experience in deep learning.
4. Experience in AI security and/or Trustworthy AI.
5. Experience in initiating and developing research plans.
6. Experience in collaborating with industry.
7. Proficient in Python.
8. Experience using PyTorch, Keras, and/or TensorFlow. Jupyter Notebook.
9. Ability to design, train and test machine learning/AI systems using appropriate methodologies and datasets.
10. Familiarity with the theory of Machine Learning fundamentals (Statistics, Optimization, Linear Algebra, Partial Derivative Equations, etc.).
11. Demonstrable commitment to the purpose and objectives of CSIT and Cyber-AI Hub.
12. Ability to assess and organise resources.
13. Evidence of being a strong communicator with excellent oral and written communication skills.
14. Demonstrate resilience and the ability to work in a fast-changing environment with competing priorities.
15. Demonstrates a high degree of integrity, honesty and openness in professional conduct.